MANUAL DE SEGURIDAD DIGITAL Y MÓVIL

PARA PERIODISTAS Y BLOGUEROS

JORGE LUIS SIERRA

FREEDOM HOUSE

ICFJ
International Center for Journalists
Advancing Quality Journalism Worldwide

MANUAL DE SEGURIDAD DIGITAL Y MÓVIL
PARA PERIODISTAS Y BLOGUEROS

Guía general para la elaboración de planes de reducción de riesgo y protocolos de seguridad digital y móvil

JORGE LUIS SIERRA

Knight International Journalism Fellow
Freedom House,
International Center for Journalists
y el Centro de Formación en Periodismo Digital
de la Universidad de Guadalajara

Octubre de 2013

1 GUÍA PARA LA ELABORACIÓN DE PLANES DE REDUCCIÓN DE RIESGO

Sección 1. Identificación de amenazas digitales y móviles 8
Sección 2. Vulnerabilidades y fortalezas de periodistas y blogueros 16
Sección 3. Definición del nivel del riesgo 18
Sección 4. Definición de objetivos y acciones a tomar 22
Sección 5. Elaboración del plan de reducción de riesgos 31

2 PROTOCOLOS Y HERRAMIENTAS DE SEGURIDAD

Elaboración de protocolos 32
Sección 6. Protección de equipos y contraseñas 34
Sección 7. Almacenamiento y protección de la información 37
Sección 8. Navegación anónima en internet 39
Sección 9. Protección de las comunicaciones digitales 41
Sección 10. Uso seguro de redes sociales 43

3 RECURSOS

Sección 11. Sitios web 44
Sección 12. Otros manuales 46

Los ejemplos mostrados en esta guía no son exhaustivos y cada usuario del manual tendrá que elaborar un plan específico de acuerdo a sus propias condiciones, amenazas y periodo por el que atraviesa. Cada seis meses realizaremos una actualización de las herramientas de seguridad digital recomendadas en este manual. A medida que la tecnología avanza rápidamente, la actualización periódica de manuales como éste resulta fundamental.

INTRODUCCIÓN

Freedom House y el International Center for Journalists (ICFJ) han unido sus fuerzas para hacer posible un proyecto que fortalezca la libertad de expresión en México a través del desarrollo de capacidades de seguridad digital de periodistas y blogueros, así como la identificación colaborativa de tendencias y patrones de agresión a través de un mapa en línea.

El Mapa de Periodistas en Riesgo (https://periodistasenriesgo.crowdmap.com) empezó a registrar incidentes a partir del 1 de diciembre de 2012, fecha en la que comenzó una nueva administración del gobierno federal.

El mapa recibe denuncias a través de un formulario en línea, correo electrónico y actualizaciones de Twitter. Los periodistas y ciudadanos que envían información lo pueden hacer de manera anónima siguiendo las instrucciones del mapa para proteger su identidad.

La creación del Mapa de Periodistas en Riesgo se ha enriquecido con experiencias colaborativas similares para registrar incidentes de crimen y corrupción en mapas de Panamá y Colombia, en un proyecto coordinador por el autor de este manual como ICFJ Knight International Journalism Fellow.

La alianza entre Freedom House y el ICFJ ha producido también un programa de entrenamiento de periodistas y blogueros en la creación de planes de reducción de riesgo y el desarrollo de herramientas de seguridad digital y móvil. El programa consiste en una fase en línea de cinco semanas a través del sitio de internet del Centro de Formación en Periodismo Digital de la Universidad de Guadalajara[1]. Después de la fase en línea, el programa sigue con una fase presencial de dos días en Guadalajara, en el que los periodistas y blogueros invitados refuerzan su dominio de las herramientas de seguridad digital y móvil e integran redes de protección y colaboración permanentes.

1 Vea http://www.centroperiodismodigital.org/sitio/

El Manual de Seguridad Digital y Móvil será una herramienta importante para reducir el riesgo de periodistas y blogueros, y mejorar las condiciones para la libertad de expresión y el periodismo de investigación. El texto también fue enriquecido por los comentarios e ideas de los periodistas y blogueros que participaron en los cursos en línea y el taller presencial de seguridad digital y móvil.

▪ ▪ ▪

El International Center for Journalists (http://icfj.org) es una organización sin fines de lucro, con sede en Washington, D.C. Su misión principal es realizar programas que usen las tecnologías más recientes para incrementar el flujo de noticias de alta calidad. Su meta es servir como catalizadores del cambio, haciendo que los socios sean más fuertes y los gobernantes más sujetos a la rendición de cuentas. Con su programa insignia, el Knight International Journalism Program (http://

www.icfj.org/our-work/knight) y por medio del Knight Fellow, el Centro ha explorado y desarrollado herramientas digitales para que periodistas y ciudadanos puedan reportar incidentes y tendencias de crimen y corrupción, y reduzcan el riesgo de sufrir ataques cibernéticos o digitales.

Freedom House (http://www.freedomhouse.org/) es una organización internacional de defensa de los derechos humanos que tiene su sede en Washington, D.C., y desarrolla una labor sistemática de defensa de la libertad de expresión a través de programas de mejoramiento del mecanismo gubernamental de protección a periodistas y defensores de los derechos humanos, así como programas de organizaciones de la sociedad civil para proteger y entrenar a periodistas y blogueros en México.

▪ ▪ ▪

En los últimos años ha sido evidente que tanto oficiales de gobierno como individuos y grupos de poder han empleado herramientas poderosas de espionaje cibernético para detectar investigaciones periodísticas que puedan afectar sus intereses o revelar actos de corrupción.

Esa dinámica ya no sólo afecta a periodistas, sino también a ciudadanos que ahora enfrentan obstáculos para usar las redes sociales en internet y las herramientas digitales para informar sobre situaciones de riesgo en comunidades afectadas por la violencia y la delincuencia organizada.

El manual ofrece al bloguero, al periodista y a las organizaciones periodísticas los elementos necesarios para que elaboren un plan general de reducción de riesgos digitales y adopten protocolos de seguridad.

Aunque existen otros manuales de seguridad disponibles, éste es el primero basado en el proceso de investigación periodística, el flujo de la información, y en los problemas intrínsecos que tiene la profesión del periodista. También es el único que provee las bases para realizar planes de reducción de riesgo.

Está pensado y basado en la experiencia de los reporteros ciudadanos. Ahora que muchas zonas de nuestros países han sufrido un silenciamiento forzado, los ciudadanos han reemplazado o, en el mejor de los casos, complementado las actividades periodísticas de medios profundamente afectados por la violencia, el chantaje, la extorsión, la amenaza y el ataque físico directo contra su personal y sus instalaciones.

Mientras otros manuales de seguridad digital están dedicados a diseminar herramientas y aplicaciones de seguridad para defensores de derechos humanos, este manual busca guiar a los periodistas y reporteros ciudadanos en la protección de sus fuentes, de su información y, a final de cuentas, de su propia integridad física, legal y psicológica.

La seguridad digital de defensores de derechos humanos y la de los periodistas tienen varios puntos en común. Sin embargo, las necesidades específicas de los periodistas y de reporteros refuerzan la importancia de:

- Usar herramientas de encriptación para mantener a salvo la información de riesgo.
- Proteger sus equipos contra virus, malware y ataques cibernéticos.
- Proteger sus datos personales en las cuentas de redes sociales.
- Proteger la comunicación móvil entre editores, reporteros, corresponsales y enviados que cubren situaciones de riesgo.
- Proteger su identidad en la navegación en internet para investigar y reportar temas de riesgo.

GUÍA PARA LA ELABORACIÓN DE PLANES DE REDUCCIÓN DE RIESGO

SECCIÓN 1
Identificación de amenazas digitales y móviles

Las amenazas a los comunicadores, sean periodistas profesionales, blogueros o reporteros ciudadanos, provienen de fuentes de naturaleza muy diversa. Pueden provenir de grupos de poder, político, económico, policíaco, militar e incluso criminal.

A pesar de su variedad, todos tienen un denominador común: son grupos cuyos intereses pueden ser afectados por la actividad del periodista. Estos grupos pueden eventualmente desarrollar el interés y la voluntad de entorpecer, detener, bloquear o eliminar la función que cumple el periodista o el ciudadano.

Por esa razón es importante distinguir entre una amenaza potencial y una real. Las formas de protección son distintas. Mientras una amenaza potencial se enfrenta a través de medidas preventivas, las amenazas reales se enfrentan usualmente con medidas correctivas, de emergencia.

Cada grupo afectado por la actividad del periodista o reportero ciudadano que tiene la capacidad de hacer daño representa una amenaza potencial. Los periodistas de investigación saben bien que su trabajo está rodeado de amenazas potenciales, pues afecta a muchas personas o grupos involucrados con actos de corrupción, violación de derechos humanos o abuso de poder.

El crimen organizado y los funcionarios involucrados en actividades corruptas siempre son amenazas potenciales para un periodista o reportero ciudadano. Esta condición obliga a los periodistas de investigación a desarrollar planes de reducción de riesgo a través de un fortalecimiento de sus capacidades profesionales, el ejercicio ético de su profesión y el seguimiento puntual de protocolos de seguridad.

En la mayoría de los casos, las amenazas ya no sólo son potenciales y se han encarnado en grupos que han cometido agresiones graves contra periodistas y ciudadanos. A pesar de que partidos de diferente doctrina han ocupado los gobiernos federales, estatales y municipales, las agresiones contra periodistas sigue siendo una tendencia creciente.

Los reporteros ciudadanos, por su parte, pueden sufrir hostigamiento de grupos criminales que piensan que los reportes les provocan un daño ("les calientan la plaza"), o de funcionarios de gobierno, molestos porque los ciudadanos revelan un clima de inseguridad que contradice las cifras oficiales.

Cuando estos grupos de poder perciben que el costo de la actividad periodística o ciudadana es muy alto, entonces desarrollan una voluntad de daño y un plan de agresión. En ese momento, dejan de ser potenciales y se convierten en amenazas reales para el periodista o el bloguero.

Esa voluntad de dañar y el plan de agresión también varía dependiendo de las circunstancias. En algunos casos, el plan de agresión

empieza por ataques digitales o campañas de desprestigio y termina en ataques físicos para dañar la integridad física o terminar con la vida del periodista o bloguero.

Según casos reportados en Chihuahua, Chiapas y Oaxaca, presuntos funcionarios públicos intentan dañar el prestigio de los periodistas a través de cuentas falsas en las redes sociales. Esas cuentas intentan dañar la credibilidad del reportero y debilitar el apoyo de sus colegas o de la sociedad, como primer paso para perpetrar después un ataque a la integridad física del periodista.

Esos grupos pueden desarrollar capacidades digitales para encontrar las vulnerabilidades de los periodistas blogueros o reporteros ciudadanos y destruir la información que tienen sobre presuntos actos de corrupción, criminalidad o violación de derechos humanos.

Algunos grupos optan por la medida directa de irrumpir en las oficinas de los medios y robarse las computadoras, discos duros y todo medio de almacenamiento digital. Los ataques recientes a las publicaciones en línea Lado B (http://ladobe.com.mx) y e-consulta (http://e-consulta.com) demuestran que los agresores buscan específicamente obtener los archivos almacenados en las computadoras y al mismo tiempo eliminar la infraestructura física para que sigan trabajando.

Otras agresiones, como el caso de los ataques cibernéticos[2] al sitio de internet de *El Mañana* de Nuevo Laredo[3], destruyen el acceso o eliminan comentarios de los usuarios que "suben" comentarios críticos del gobierno local[4].

Reporteros de Chihuahua denunciaron por ejemplo la creación de cuentas con identidad falsa en Facebook[5] para espiar y conocer detalles de la vida privada de los periodistas de la región. Ese tipo de ataque ha sido frecuente en otros estados y tiene como fin hostigar y buscar información sobre las vulnerabilidades de los periodistas y blogueros.

Tanto gobernantes como grupos criminales están desarrollando capacidades de espionaje sobre periodistas y blogueros independientes que no controlan. Esa capacidad tecnológica ha sido acompañada de planes concretos de agresión que incluyen, al menos en un caso reportado en Chiapas, la contratación de expertos de tecnologías de espionaje.

AMENAZAS

Entendemos como amenazas la existencia de individuos o grupos de poder que puedan resultar afectados por el trabajo del periodista, del bloguero o del reportero ciudadano, y que tienen la capacidad para causar un daño físico, psicológico, legal o digital. Estas amenazas dejan de ser potenciales y pasan a ser reales cuando desarrollan la voluntad de causar daño y trazan un plan para producirlo.

Para conocer bien a las amenazas debemos contar con información detallada de ellas:

- Nombre
- Capacidades (número de personas, armas que manejan, tecnología de espionaje)
- Fortalezas (apoyo de gobernantes corruptos)
- Debilidades (rivalidades con otros grupos de poder, sensibilidad ante denuncias públicas)
- Voluntad de dañar

2 Ver: https://periodistasenriesgo.crowdmap.com/reports/view/55
3 http://elmanana.com.mx/
4 Ver entrevista con Daniel Rosas, editor de *El Mañana* de Nuevo Laredo. YouTube, 23 de mayo de 2013. https://www.youtube.com/watch?v=KqE5QDQEbD8
5 Ver denuncia en Facebook: https://www.facebook.com/photo.php%3Ffbid=10151538028491178%26set=a.83785416177.78176.666686177%26type=1%26theater y también el reporte en el Mapa de Periodistas en Riesgo: https://periodistasenriesgo.crowdmap.com/reports/view/43

Estos podrían ser algunos ejemplos de amenazas potenciales:

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Narcotraficantes, funcionarios públicos vinculados con narcotraficantes	▪ Unidades operativas armadas ▪ "Halcones" o monitores callejeros ▪ Uso de espías en las redacciones ▪ Corrupción de policías, militares o funcionarios locales ▪ Equipo de vigilancia electrónica ▪ No son susceptibles a la presión política	▪ Asesinato o desaparición ▪ Golpes severos ▪ Amenazas de muerte ▪ Ataque con armas de fuego contra medios ▪ Secuestro ▪ Órdenes forzadas de inserción o silencio
Funcionarios públicos involucrados con esquemas de corrupción	▪ Unidades operativas ▪ Corrupción de reporteros, editores o directivos ▪ Uso de espías en las redacciones ▪ Uso ilegal de sistemas de inteligencia oficial ▪ Equipo de vigilancia electrónica ▪ Contratación de "sicarios"	▪ Asesinato o desaparición ▪ Golpes severos ▪ Amenazas de muerte ▪ Secuestro ▪ Allanamiento de oficinas y robo de equipos ▪ Agresión legal con demandas civiles o penales
Empresas privadas involucradas en esquemas de corrupción	▪ Corrupción de reporteros, editores o directivos ▪ Uso de sistemas de inteligencia privada ▪ Equipo de vigilancia electrónica ▪ Despachos jurídicos	▪ Junto con funcionarios corruptos, estas empresas pueden participar o financiar ataques físicos contra periodistas y blogueros ▪ Hostigamiento legal con demandas civiles o penales

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Grupos paramilitares	▪ Células operativas armadas ▪ Colusión con policías, militares o funcionarios locales ▪ Control territorial	▪ Ataques armados contra periodistas y blogueros
Movimientos armados	▪ Células operativas armadas ▪ Control territorial	▪ Ataques armados contra periodistas y blogueros
Pandillas	▪ Células operativas armadas	▪ Ataques armados contra periodistas y blogueros
Multitudes enardecidas	▪ Concentración masiva de personas dispuestas a la acción	▪ Ataque físico contra periodistas y blogueros ▪ Robo de equipos
Grupos antimotines	▪ Fuerza de choque organizada	▪ Ataque físico contra periodistas y blogueros ▪ Detención arbitraria ▪ Robo de equipos

AMENAZAS DIGITALES

Las amenazas digitales provienen de grupos de poder interesados en conocer la información que posee un periodista, impedir que tenga acceso a esa información o destruirla. El experto Dimitri Vitaley (2007) considera que este tipo de amenazas representan la posibilidad de que un individuo dañe la integridad de nuestras computadoras, la información almacenada en ellas y las comunicaciones en línea que sostenemos. El autor cita como ejemplos de amenaza digital a los virus cibernéticos, la confiscación de la computadora y el bloqueo del sitio web. Con el crecimiento de la tecnología, el ataque puede ser dirigido a dispositivos móviles como teléfonos celulares, laptops y tabletas.

Estas podrían ser ejemplos de amenazas digitales potenciales para periodistas y blogueros:

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Gobiernos	▪ Adquisición y desarrollo de tecnología, herramientas digitales y cibernéticas para acopio de información, actividades de, vigilancia, espionaje y sabotaje digital. ▪ Acopio masivo de datos y comunicaciones privadas por medios digitales. ▪ Monitoreo de la actividad en línea y las comunicaciones digitales de individuos, organizaciones, instituciones, grupos armados y organizaciones criminales. ▪ Sostenimiento de "ejércitos" de *trollers* que irrumpen en las redes sociales o espacios digitales para desvirtuar o distraer la discusión pública.	▪ Filtrado de internet. Bloqueo de información en internet que contradice los objetivos gubernamentales. ▪ Bloqueo *just-in-time*. Bloqueo del acceso a información durante convulsiones políticas y manifestaciones de descontento social. ▪ Denegación de servicio. Bloqueo del acceso a un sitio o página web por medio de una o varias computadoras. ▪ *Defacement* (Desfiguración del rostro. Eliminación y sustitución del contenido de un sitio web o página de internet . ▪ Campañas de propaganda por vías digitales en línea en contra de medios de comunicación, periodistas o blogueros. ▪ Vigilancia electrónica de periodistas, blogueros o medios de comunicación. ▪ Ataques dirigidos con programas maliciosos (*malware*). ▪ Promoción de regulaciones y leyes de control de internet y de usuarios de redes sociales. ▪ Confiscación o robo de computadoras. ▪ Campañas de desprestigio contra periodistas y blogueros por redes sociales.

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Narcotraficantes, grupos de la delincuencia organizada y funcionarios públicos vinculados con narcotraficantes	▪ "Halcones" o monitores digitales. ▪ Monitoreo de la actividad en línea y las comunicaciones digitales. ▪ Adquisición y desarrollo de tecnología, herramientas digitales y cibernéticas para espionaje. ▪ Adquisición de equipo para interceptación de datos y comunicaciones digitales. ▪ Uso de redes sociales y blogs para sembrar terror y diseminar información favorable.	▪ Espionaje de la actividad en línea o comunicaciones digitales. ▪ Lanzamiento de amenazas de muerte contra periodistas y blogueros por vías digitales. ▪ Censura directa de medios de información digitales. ▪ Intento de geolocalización (ubicación física) de periodistas y blogueros. ▪ Acopio masivo de información para detectar la presencia de blogueros o periodistas cercanos a las situaciones de riesgo. ▪ Órdenes forzadas de inserción o silencio en medios en línea. ▪ Confiscación o robo de computadoras y dispositivos móviles de periodistas y blogueros.
Funcionarios públicos involucrados con esquemas de corrupción	▪ Monitoreo de la actividad en línea y las comunicaciones digitales. ▪ Adquisición y desarrollo de tecnología, herramientas digitales y cibernéticas para espionaje. ▪ Adquisición de equipo para interceptación de datos y comunicaciones digitales. ▪ Sostenimiento de "ejércitos" de *trollers*.	▪ Espionaje de la actividad en línea o comunicaciones digitales. ▪ Lanzamiento de amenazas de muerte contra periodistas y blogueros por vías digitales. ▪ Censura directa de medios de información digitales. ▪ Campañas de desprestigio contra periodistas y blogueros por redes sociales. ▪ Confiscación o robo de computadoras y dispositivos móviles de periodistas y blogueros.

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Empresas privadas involucradas en esquemas de corrupción	▪ Monitoreo de la actividad en línea y las comunicaciones digitales. ▪ Adquisición y desarrollo de tecnología, herramientas digitales y cibernéticas para espionaje. ▪ Adquisición de equipo para interceptación de datos y comunicaciones digitales.	▪ Espionaje de la actividad en línea o comunicaciones digitales. ▪ Junto con funcionarios corruptos, estas empresas pueden participar o financiar ataques digitales contra sitios o páginas web de periodistas y blogueros. ▪ Robo de computadoras y dispositivos móviles de periodistas y blogueros.
Operadores de *Botnets* (creadores de redes de computadoras "zombie" usadas para distribuir programas maliciosos, robar información u organizar ataques de denegación de servicio)	▪ Ofrecimiento de servicios de creación de *botnets* o renta de servidores para distribuir programas maliciosos y lanzar ataques de denegación de servicio.	▪ Contratados por otros grupos de poder, pueden ayudar a lanzar ataques digitales contra medios, periodistas y blogueros.
Crackers	▪ Desarrollo de conocimientos y uso práctico de tecnologías de ataque digital.	▪ Contratados por otros grupos de poder, pueden lanzar ataques digitales contra medios, periodistas y blogueros. ▪ Ataques contra sitios o páginas informativas como parte de ritos de iniciación o prácticas de técnicas de crackeo.

Grupo de poder	Capacidades de dañar	Voluntad de dañar a periodistas o blogueros
Trollers	▪ Grupos de operadores de cuentas ficticias para sembrar rumor o desvirtuar la discusión pública.	▪ Contratados por otros grupos de poder, lanzan y operan campañas de desprestigio contra periodistas y blogueros.
Phishers	▪ Capacidades para ejecutar operaciones de engaño para *crackear* cuentas y obtener información privada y confidencial de periodistas y blogueros.	▪ Contratados por otros grupos de poder, dirigen ataques de *phishing* contra periodistas y blogueros.
Spammers	▪ Desarrollan equipos de tecnólogos que diseminan desinformación, programas maliciosos, ataques de *phishing* o campañas de desprestigio por medio del envío de llamadas telefónicas, correos electrónicos o mensajes de texto no solicitados.	▪ Contratados por otros grupos de poder, lanzan campañas para influir, desprestigiar o contrarrestar la opinión de periodistas y blogueros.

SECCIÓN 2
Vulnerabilidades y fortalezas de periodistas y blogueros

VULNERABILIDADES

La magnitud del daño hacia la información de un periodista o reportero ciudadano depende de qué tanta fortaleza o debilidades tengan estos últimos. Mientras más fuerte es la amenaza y más débil el periodista, la magnitud del daño y la naturaleza del ataque pueden ser mayores.

Un bloguero o periodista, por ejemplo, que tenga una sola contraseña para todas sus cuentas o varias de ellas, puede ser altamente vulnerable y sufrir la pérdida de toda su información si un *cracker* descubre la contraseña y entra con facilidad a todas sus cuentas. En cambio, un periodista que crea diferentes contraseñas largas (más de 15 caracteres) y las fortalece con mayúsculas, minúsculas, números y signos de puntuación puede perder menos información en caso de un ataque digital o cibernético.

Los reporteros que se comunican con sus editores a través de correos electrónicos inseguros, chats no encriptados, o que mezclan datos personales con información de riesgo, suelen ser más vulnerables ante ataques digitales.

Esos factores de debilidad contribuyen a que la magnitud del daño ocasionado por un ataque sea más grave. Algunos de los factores de debilidad pueden ir desde hábitos personales inseguros, falta de equipo, descuido empresarial, crisis personales, falta de entrenamiento o preparación, carencia de planes. Suelen hallarse múltiples factores de debilidad en editores que envían a reporteros inexpertos o sin contactos a cubrir un incidente de alto riesgo, reporteros o fotógrafos que llegan antes que las fuerzas de seguridad a lugares donde se ha cometido un crimen, periodistas que viajan con todos sus archivos completos sin encriptar en las laptop, memorias USB o equipos móvies, o reporteros que escriben sus notas sin verificar lo suficiente la información de alto riesgo.

En terreno de las vulnerabilidades digitales o móviles, éstas pueden ir desde la existencia de contraseñas débiles, la falta de actualización en los programas de cómputo, la falta de dominio o de conocimiento de herramientas de seguridad mínimas, la mezcla de información profesional con datos personales en línea, el almacenamiento de listas de contactos en archivos sin encriptar, la carencia de programas antivirus en las computadoras, etcétera.

Vitaliev se refiere a las vulnerabilidades como el grado en el que uno es susceptible a la pérdida, daño y sufrimiento en el caso de un ataque y añade que, usualmente, las vulnerabilidades en el campo de la tecnología se originan en la falta de comprensión o de entrenamiento.

Estos serían algunos ejemplos de vulnerabilidades digitales:

- El periodista usa la misma contraseña para todas sus cuentas.
- Las contraseñas del periodista son de ocho caracteres y no tienen signos de puntuación.
- El reportero sólo tiene una batería que frecuentemente se descarga para su celular o laptop y debe usar teléfonos y computadoras de salas de prensa oficiales.
- El periodista olvida cerrar su cuenta en computadoras o teléfonos prestados.
- La computadora del periodista no tiene protector de pantalla.
- La computadora tiene archi-

vos y fotos personales del periodista.
- El periodista usa Whatsapp para comunicarse con sus fuentes.
- El periodista lleva todos sus contactos almacenados en su teléfono celular.
- Ningún documento confidencial está encriptado en la computadora del periodista.
- El periodista abre vínculos activos en correos o mensajes provenientes de fuentes desconocidas o de baja confianza.

FORTALEZAS O CAPACIDADES

Las fortalezas nos ayudan a disminuir la probabilidad de que ocurra un ataque o, en el peor de los casos, de reducir el daño que nos ocasione. Normalmente, las fortalezas de un periodista consisten en el ejercicio profesional de su labor, el seguimiento de estándares elevados y la insistencia en lograr información confirmada, contextualizada y "blindada". Nada le garantiza a los periodistas o blogueros la seguridad completa de que no van a ser víctimas de un ataque u objeto de un plan de agresión. Sin embargo, las oportunidades para atacarlo pueden ser reducidas mediante el comportamiento profesional permanente por parte del periodista.

En las condiciones actuales de la delincuencia organizada y la corrupción de muchas esferas del gobierno, el periodista y el reportero ciudadano necesitan otras fortalezas adicionales como la protección de círculos de confianza, redes u organizaciones formales de defensa de la libertad de expresión. Aunque en sentido estricto un periodista no es un defensor de derechos humanos, su trabajo sí lo acerca a las redes de derechos humanos que comparten intereses y pueden eventualmente protegerlo.

Esas fortalezas, que en el campo digital se vuelven capacidades, son todos aquellos factores o recursos que contribuyen a reducir la magnitud del daño o la probabilidad de un ataque. Pueden ser de una índole muy variada. Entre ellos pueden estar la existencia de una estrategia bien definida de reducción de riesgos, la planeación detallada de coberturas de alto riesgo, la comunicación adecuada entre editores y reporteros, el apoyo empresarial, la experiencia acumulada del periodista. En el plano digital pueden mencionarse el acceso a redes de internet seguras, la elaboración de contraseñas fuertes, el entrenamiento en el uso de herramientas digitales, equipos de tecnología avanzada y el desarrollo de protocolos de seguridad.

Algunos ejemplos de fortalezas en el campo de la seguridad digital podrían ser:
- Todas las contraseñas que usa el periodista son mayores de 15 caracteres y mezclan mayúsculas, minúsculas, números y signos de puntuación.
- Cada cuenta del periodista tiene una contraseña distinta que actualiza periódicamente.
- El periodista usa Gibberbot, una herramienta para encriptar mensajes instantáneos, para comunicarse con sus fuentes. Ver: https://guardianproject.info/apps/gibber/
- Los archivos más sensibles del periodista están guardados en carpetas encriptadas.
- El periodista evita subir información personal en sus cuentas de Twitter y Facebook
- El reportero ciudadano usa Tor para navegar mientras sube información sobre situaciones de riesgo a Twitter. Ver: https://www.torproject.org
- El periodista usa riseup.net, el servicio de correo electrónico que encripta los mensajes electrónicos mientras viajan por la web hacia su destinatario.

SECCIÓN 3
Definición del nivel del riesgo

El nivel de riesgo debe ser entendido como una interacción entre la amenaza y las vulnerabilidades y fortalezas. Cuando la amenaza es muy grande y las vulnerabilidades son muchas, entonces podríamos afirmar que el riesgo es grande y probable. La vulnerabilidad multiplica la probabilidad de que la amenaza use sus capacidades y planifique un ataque contra la integridad del periodista o reportero ciudadano.

En algunos casos de agresión registrados en los últimos años en México, el periodista que se muda de una ciudad a otra para trabajar, pierde temporalmente las fortalezas que le dan la red de apoyo, la existencia de contactos que le pueden ayudar rápidamente y el conocimiento del contexto de su ciudad de origen. Además de perder esas fortalezas, los periodistas en esas condiciones incrementan sus vulnerabilidades si viven solos, no crean círculos de confianza o redes de apoyo mutuo de manera rápida, y si comienzan a trabajar sin comprender el contexto y la proximidad de las líneas de riesgo.

Lo mismo sucede con los periodistas que son enviados a cubrir una crisis de seguridad a otro estado. Las comunicación con su organización, fuentes de información y redes de apoyo puede sufrir una limitación drástica en condiciones de gran actividad criminal o de operaciones intensas de las fuerzas de seguridad. Si el periodista no está familiarizado con la zona y carece de fuentes o contactos de confianza, su labor será más difícil y su nivel de riesgo mayor.

Para compensar esas debilidades temporales, el periodista puede ser entrenado previamente a cubrir situaciones de alto riesgo y establecer protocolos de comunicación con sus editores.

Riesgo = Amenaza x vulnerabilidad

En cambio la existencia de capacidades o fortalezas puede disminuir el riesgo como lo presenta la fórmula siguiente:

Riesgo = Amenaza x vulnerabilidad /capacidades

Al evaluar la amenaza, debemos determinar si su capacidad y voluntad de dañar ponen en riesgo alguna de las condiciones de integridad del individuo o grupo afectado.

Integridad en riesgo		Daño a la integridad física	Daño a la integridad psicológica	Daño a la integridad digital
Magnitud del daño	Nivel de riesgo			
Catastrófica	**Extremo**	▪ Muerte	▪ Severo	▪ Pérdida total definitiva
Severa	**Muy alto**	▪ Lesión no remediable	▪ Severo	▪ Pérdida parcial definitiva
Alta	**Alto**	▪ Lesión remediable en el largo plazo	▪ Moderado	▪ Recuperable en el largo plazo
Mediana	**Mediano**	▪ Lesión remediable en el mediano plazo	▪ Moderado	▪ Recuperable en el mediano plazo
Leve	**Bajo**	▪ Lesión remediable en el corto plazo	▪ Bajo	▪ Recuperable en el corto plazo

La segunda manera de evaluar el riesgo es comparando la probabilidad de ocurrencia con la magnitud del daño.

Si la magnitud es catastrófica, pero la probabilidad de que ocurra es muy lejana, entonces el nivel de riesgo es bajo. Caso contrario, cuando la magnitud sigue siendo catastrófica, pero la probabilidad de ocurrencia es inminente, entonces el nivel de riesgo es extremo.

Probabilidad / Magnitud	Inminente	Muy cercana	Cercana	Lejana	Muy lejana
Catastrófica	▪ Extremo	▪ Extremo	▪ Alto	▪ Medio	▪ Bajo
Severa	▪ Extremo	▪ Extremo	▪ Alto	▪ Medio	▪ Bajo
Alta	▪ Alto	▪ Alto	▪ Alto	▪ Medio	▪ Bajo
Mediana	▪ Medio	▪ Medio	▪ Medio	▪ Medio	▪ Bajo
Leve	▪ Bajo	▪ Bajo	▪ Bajo	▪ Bajo	▪ Bajo

Como es muy difícil tener una situación de no riesgo, porque esa es prácticamente inexistente, debemos seguir adelante con el reconocimiento y aceptación de un nivel de riesgo determinado.

La aceptación depende también de cada nivel de riesgo y también de las condiciones de cada persona y organización. En términos generales, los niveles bajo y medio de riesgo tienden a ser aceptables para los periodistas o reporteros ciudadanos que reportan incidentes de crimen, corrupción, abusos de poder y violación a los derechos humanos. Prácticamente, ya ningún periodista reporta estar en un nivel bajo de riesgo. Aquellos temas de cobertura supuestamente de bajo riesgo como Deportes o Espectáculos, dejaron de serlo ya sea por la corrupción existente en esos campos, o por la penetración del narcotráfico y el control de la delincuencia organizada.

Los periodistas trabajan entonces en situaciones que van del riesgo medio al alto y se ven obligados a aceptar las condiciones de riesgo para seguir trabajando.

Aunque los niveles de riesgo alto y extremo tienden a ser inaceptables, algunos periodistas deben seguir adelante. Eso implica la obligación de las empresas, y en su caso del propio periodista, de prepararse más para cubrir situaciones de riesgo, crear planes adecuados de reducción del riesgo y seguir rigurosamente los protocolos de seguridad. La tarea principal de un periodista en una situación de alto riesgo es evitar caer de manera voluntaria o involuntaria en una situación de riesgo extremo donde la magnitud del daño puede ser catastrófica y la probabilidad de que ocurra, muy cercana.

Sólo en el nivel de riesgo extremo, cuando la magnitud del daño puede ser catastrófica y la probabilidad de ocurrencia inminente, la actividad que esté realizando el periodista o el bloguero debe ser suspendida de inmediato. La frase famosa de que "no hay historia que valga una vida" se refiere fundamentalmente a la condición inaceptable del nivel de riesgo extremo.

Nivel de riesgo	Nivel de aceptabilidad	Tipo de medidas	Temas para corregir si el riesgo incrementa
Extremo	▪ Inaceptable	▪ Suspensión inmediata	▪ Estrategias fallidas
Alto	▪ Inaceptable	▪ Protocolo de reacción	▪ Protocolos fallidos
Medio	▪ Aceptable	▪ Protocolo de prevención	▪ Protocolos insuficientes
Bajo	▪ Aceptable	▪ Protocolo de prevención	

Las medidas a adoptar también tienen que ver con el nivel de riesgo y con las capacidades de cada persona y organización. El paso de un nivel de riesgo a otro puede ser un indicativo de que algo ha fallado en las políticas de reducción de riesgo.

Las medidas preventivas (también conocidas como protocolos de seguridad) sirven, por ejemplo, para impedir que pasemos del nivel bajo o medio de riesgo al nivel alto. Sin embargo, si pasamos al nivel alto de riesgo, las medidas preventivas pueden haber fracasado o haber sido mal elegidas y urge tomar medidas correctivas para bajar el nivel de riesgo.

En el caso de que estemos en un nivel de riesgo extremo, es posible que nuestras estrategias generales, y no sólo las medidas preventivas, hayan sido inadecuadas y sea necesaria una suspensión inmediata de la operación para evitar en lo posible el daño catastrófico.

Rosalía Orozco, directora del Centro de Formación de Periodismo Digital de la Universidad de Guadalajara.

SECCIÓN 4
Definición de objetivos y acciones a tomar

Luego de determinar el nivel de riesgo en el que nos encontramos, estamos en la necesidad de definir los objetivos y las acciones a emprender para reducir el riesgo o evitar que se incremente.

Los objetivos deben depender del análisis de las amenazas, debilidades y fortalezas propias de cada organización periodística y de cada periodista o reportero ciudadano individual. Lo que sirve para un periódico, puede ser que no sea útil para un canal de televisión o para una publicación en línea. Lo que funciona para un reportero de la fuente policiaca, puede ser que no funcione para un reportero que cubre política o negocios.

Esos objetivos deben corresponder al contexto donde trabaja el periodista y, también, al momento por el que atraviesa. Los objetivos de seguridad de un periodista que trabaja en Ciudad Juárez pueden ser muy distintos del que tiene uno que trabaja en Veracruz, Guerrero o Baja California. Si un periodista viaja del Distrito Federal para cubrir un conflicto intercomunitario en Oaxaca, sus objetivos deben definirse de acuerdo con la situación que prevalezca en esas comunidades en el momento de su llegada.

Lo mismo sucede con periodistas que van a cubrir situaciones de alto riesgo en otros países. Aunque las situaciones sean similares (actividad de pandillas, asesinatos del narcotráfico, enfrentamientos armados), los contextos pueden ser diferentes. Lo que en un país significa seguridad, en otro puede representar riesgo. De ahí que los protocolos tengan que estar basados en el análisis de las amenazas en el contexto real y en la evaluación de las fortalezas y vulnerabilidades propias.

Las circunstancias dinámicas nos obligan a revisar los protocolos constantemente. La geografía del riesgo cambia incesantemente, las amenazas pueden ganar o perder capacidades y el lugar que ocupa un plan de agresión contra un periodista o bloguero puede cambiar de jerarquía. Eso sucede por ejemplo en las ciudades, poblados o municipios donde grupos rivales de la delincuencia organizada se disputan con violencia extrema el control de la localidad.

Aunque los periodistas deben mantenerse ajenos e imparciales durante al conflicto, es una necesidad imperativa conocer y evaluar a cada momento la correlación entre las fuerzas en choque. El asesinato de un narcotraficante que lanzó amenazas de muerte a periodistas, por ejemplo, no significa que la situación amenazante ha desaparecido. Lo mismo puede suceder con funcionarios corruptos que son sentenciados a penas de prisión. El ex gobernante en prisión puede ser incluso una amenaza mayor por su voluntad de venganza.

DEFINICIÓN DE OBJETIVOS

Los objetivos de una estrategia de reducción de riesgo deben ser redactados de tal manera que su cumplimento sea medible y factible. Es más medible un objetivo como "Fortalecer todas las contraseñas al cien por ciento" que "aumentar la seguridad de mis cuentas de redes sociales". Lo factible también es importante. Es más factible redactar el objetivo de "Usar una cuenta de correo electrónico encriptado gratuito" que "Usar la versión profesional de Hushmail

para incrementar la seguridad de mis mensajes electrónicos".

Esos objetivos apuntan fundamentalmente hacia la reducción del nivel de riesgo por medio de una disminución de las vulnerabilidades y de un aumento de las capacidades o fortalezas.

En el primer caso: "Fortalecer todas las contraseñas al 100 por ciento", el periodista cambia las contraseñas inseguras y eso le posibilita eliminar debilidades.

Al redactar tus objetivos, también deberás jerarquizar adecuadamente las amenazas que enfrentas y anotar con detalle las vulnerabilidades y fortalezas que correspondan a cada amenaza. Recuerda que no es posible enfrentar todas las amenazas al mismo tiempo ni resolver todas las vulnerabilidades existentes. Sin embargo, la identificación adecuada de las amenazas a enfrentar, la definición exacta de nuestras vulnerabilidades y capacidades nos ayudarán a reducir el riesgo de manera cada vez más eficiente.

Estos podrían ser ejemplos de objetivos seguido de acciones concretas para cumplir con ellos:

Objetivos	Acciones a tomar	Impacto en la organización
Establecer un sistema de evaluación del riesgo como parte de la planificación de la cobertura.	▪ Evitar la cobertura de riesgo extremo y planificar las coberturas de alto riesgo. ▪ Elaborar un protocolo de seguridad para toda la organización periodística ▪ Entrenar a todo el personal en Cobertura Segura y Seguridad Digital.	▪ Creación de un comité de seguridad que audite el riesgo de la empresa periodística y elabore protocolos de prevención y emergencia.
Cubrir una crisis de seguridad (por ejemplo, la matanza masiva de inmigrantes en San Fernando, la captura o muerte de un jefe de narcotraficantes).	▪ Contar con un protocolo de seguridad que permita disminuir el riesgo de los reporteros asignados a cubrir esa información. ▪ Conseguir apoyo de reporteros experimentados. ▪ Contar con sistemas de comunicación seguros.	▪ Crear una red de solidaridad entre periodistas y blogueros.
Crear un canal de comunicación seguro entre el editor y los reporteros que cubren situaciones de alto riesgo.	▪ Entrenar a editores a reporteros en el uso de herramientas de seguridad en la comunicación.	▪ Diseñar un protocolo de seguridad en las comunicaciones entre editores y reporteros.

Ya que has evaluado tus niveles de riesgo en el uso de computadoras, equipos móviles, contraseñas, manejo de documentos confidenciales en formato digital, navegación en internet, comunicación en línea, uso de blogs y de redes sociales, puedes ensamblar un solo documento que contenga los objetivos del plan de seguridad, las medidas necesarias que serán adoptadas, y una estimación de los recursos necesarios para reducir el riesgo existente.

La siguiente tabla es un ejemplo de cómo podemos hacer un esquema de nuestros retos en materia de seguridad general de periodistas y blogueros:

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Eliminar a reporteros que "están con el enemigo", "calientan la plaza" o no "siguen órdenes"	▪ Sí, tiene comprada a la policía local, tiene informantes en el medio de comunicación, no hay despliegue de autoridades federales	▪ Es enviado a otro estado, y está aislado, la cobertura, no está planificada, no conoce bien el terreno, no tiene fuentes ni redes de solidaridad en la zona.	▪ Profesional y ético, la empresa lo apoya, pero le exige que cumpla la asignación.	▪ Extremo, riesgo de daño muy grave.	▪ Establecer un sistema de evaluación del riesgo como parte de la planificación de la cobertura.	▪ Evitar la cobertura en esas condiciones y esperar hasta planificar. ▪ Si editores y reporteros deciden seguir adelante con la cobertura, valorar la necesidad de protección dura.

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Eliminar a reporteros que "están con el enemigo", "calientan la plaza" o no "siguen órdenes".	▪ Sí, tiene bajo su control a autoridades locales y también goza de apoyo de funcionarios federales que le dan protección.	▪ Aislado, recién ha llegado a trabajar en la ciudad, no conoce bien el terreno, no tiene redes de solidaridad, la empresa es ambigua y no apoya lo suficiente.	▪ Tiene poca experiencia pero es muy ético y profesional.	▪ Extremo, riesgo de daño muy grave.	▪ Fomentar las redes de solidaridad, conseguir apoyo de reporteros experimentados.	▪ Planificar al máximo las coberturas, especialmente si están relacionadas con actos del crimen organizado. ▪ Conseguir entrenamiento, valorar el cambio de medio, o posiblemente la salida de la ciudad.

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Está dispuesto a eliminar al periodista específico por la cobertura reciente de los hechos de violencia. Un grupo rival quiere desestabilizar la ciudad para obligar a los efectivos federales a lanzarse contra sus rivales.	▪ Sí, tiene a las autoridades locales de su parte, pero está luchando contra narcos rivales y hay una presencia importante de soldados y policías federales que patrullan la ciudad, se han registrado enfrentamientos entre autoridades y bandas criminales.	▪ Vive solo o sola, en un barrio aislado, aunque sabe que otros colegas han sido asesinados recientemente, desconoce si hay alguna acción en curso para agredir su persona.	▪ Tiene experiencia, está en contacto con redes de apoyo en el D.F., es muy profesional y la empresa lo apoya, pero insiste en mantener la cobertura.	▪ Extremo, riesgo de daño muy grave.	▪ Establecer mecanismos de emergencia cuando hay agresiones graves a periodistas en la localidad, crear un mecanismo para valorar el nivel de riesgo de los reporteros, tender un vínculo con autoridades federales.	▪ Hablar con los editores, tratar de valorar el riesgo en la ciudad. Mudarse de vivienda, exigir el apoyo gubernamental, valorar la necesidad de protección dura, promover el apoyo público.

Esta es una tabla con ejemplos de objetivos y acciones de seguridad digital:

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Eliminar información comprometedora almacenada en la computadora del periodista o del bloguero.	▪ Sí. Sus células son capaces de irrumpir en una redacción o casa particular para robar o destruir el equipo que contiene la información.	▪ La computadora carece de contraseñas, hay acceso relativamente fácil a la oficina. No hay copia de seguridad de la información. La información no está codificada.	▪ Buena comunicación entre reportero y editor.	▪ Extremo, riesgo de daño muy grave	▪ Proteger la información de un reportaje sobre corrupción de autoridades locales y vínculos con delincuencia organizada.	▪ Establecer reglas de acceso a la oficina. Equipar la computadora con contraseñas. Codificar la información. Guardar una copia de respaldo fuera de la oficina.

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Conocer la información que maneja el periodista o bloguero a través de la vigilancia de su actividad en internet.	▪ Sí, expertos en informática al servicio de un funcionario corrupto buscan vigilar la actividad en internet del periodista o bloguero.	▪ El periodista usa navegadores inseguros y en ocasiones trabaja y envía sus notas por correo electrónico desde cafés internet cuando está cubriendo eventos.	▪ Suele trabajar en equipos protegidos por cortafuegos (*firewalls*) en su oficina. ▪ Utiliza el programa outlook para comunicarse con sus fuentes y editores.	▪ El nivel de riesgo es medio mientras trabaja en la oficina, pero se eleva a nivel alto cuando acude a cafés internet para escribir sus notas y enviar su información.	▪ Mejorar los hábitos de seguridad en la navegación en internet mientras escribe sus notas para su medio o entradas para su blog.	▪ Enviar sus notas sólo a través de servicios de correo electrónico protegidos con el prefijo https. ▪ Usar de preferencia navegadores Firefox o Chrome. ▪ Descontinuar el uso de Internet Explorer. Evitar el uso de los mismos cafés internet para trabajar mientras está fuera de la oficina. ▪ Usar acceso inalámbrico a internet a través de modems USB.

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Robar el teléfono celular	▪ Sí, un grupo está dedicado a robar celulares en la vía pública o en medios de transporte publico.	▪ El teléfono contiene datos personales y de trabajo. No tiene habilitado ningún PIN, patrón o contraseña. Las contraseñas del correo electrónico están almacenadas en el teléfono. Todos los contactos con las fuentes están almacenados.		▪ Nivel alto, riesgo de pérdida del celular por robo. Si la información cae en manos de grupos criminales, puede haber riesgo para las fuentes y el propio periodista.	▪ Proteger la información del celular y reducir el impacto negativo en caso de robo o pérdida del equipo.	▪ Proteger el celular con contraseñas, PIN o patrones. ▪ Borrar información personal que pueda comprometer la seguridad del periodista o blogguero. ▪ Memorizar datos de contacto con fuentes confidenciales. ▪ Contratar un programa para eliminar la información o localizar el aparato a control remoto.

Crimen organizado		Periodista		Riesgo	Estrategia	
Voluntad	Capacidad	Vulnerabilidad	Fortaleza	Nivel	Objetivos	Acciones
▪ Ubicar físicamente a un periodista o bloguero para preparar un ataque en su contra	▪ Sí. Un equipo de ingenieros en computación, al servicio de un oficial corrupto o un grupo criminal intentan conocer el IP del usuario para geolocalizarlo.	▪ El periodista utiliza servicios de correo electrónico que no ocultan el IP del usuario. Desde esa cuenta pide y envía información a fuentes confidenciales que posiblemente estén vigiladas.	▪ El periodista ha labrado muy bien la relación con las fuentes confidenciales, pero sigue utilizando cuentas inseguras para comunicarse con ellas.	▪ Nivel alto o extremo. El equipo técnico está trabajando rápidamente para indagar el IP del usuario y está interceptando sus correos electrónicos.	▪ Proteger el IP del usuario para impedir que sea geolocalizado.	▪ Suspender el uso de las cuentas de correo electrónico inseguras y usar Gmail para fines profesionales. ▪ Usar anonimizadores del IP en la navegación por internet y sacar una cuenta alternativa por medio de la plataforma TOR.

SECCIÓN 5
Elaboración del plan de reducción de riesgos

En la redacción del plan general de reducción de riesgo es importante que se haga una valoración adecuada de lo siguiente:

- Amenazas potenciales y reales (capacidades, voluntad de daño y plan de agresión).
- Tus vulnerabilidades.
- Tus fortalezas o capacidades.
- Los recursos con los que cuentas.

Ese análisis te va a permitir definir los objetivos de tu plan y jerarquizar los riesgos que enfrentas. Algunos serán aceptables y otros no, todo dependerá del nivel de riesgo, la naturaleza de las amenazas y tus propias fortalezas y vulnerabilidades.

Puedes seguir un ejemplo como el siguiente:

PLAN GENERAL DE REDUCCIÓN DE RIESGOS

I. OBJETIVOS

Objetivo general:

Reducir los niveles de riesgo en materia física, psicológica y digital mediante el fortalecimiento de las capacidades y la disminución de las vulnerabilidades del periodista, bloguero o reportero ciudadano.

Objetivos particulares de seguridad física:

- Establecer un sistema de evaluación del riesgo como parte de la planificación de coberturas de alto riesgo.
- Fomentar las redes de solidaridad en el municipio.
- Conseguir apoyo de reporteros experimentados de la localidad.

Objetivos particulares de seguridad digital:

- Organizar y encriptar la información de reportajes, blogs y actividad en redes sociales sobre corrupción de autoridades locales y vínculos con delincuencia organizada.
- Encriptar discos duros para proteger la información almacenada en equipos de cómputo.
- Borrar en forma segura información confidencial de dispositivos móviles como celulares y tabletas.
- Introducir programas de rastreo para reducir el impacto negativo en caso de robo o pérdida del equipo fijo o móvil.
- Mejorar los hábitos de seguridad en la navegación en internet mientras el periodista, bloguero o reportero ciudadano escribe sus notas o entradas para su blog.
- Proteger el IP del usuario para impedir que sea geo-localizado y sea víctima de un ataque planificado en su contra.

Acciones a tomar:

- En caso de riesgo alto o extremo, exigir la protección gubernamental, valorar la necesidad de protección dura y convocar el máximo apoyo público posible.
- Planificar al máximo las coberturas, especialmente si están relacionadas con actos del crimen organizado.
- Conseguir entrenamiento, valorar el cambio de medio, o posiblemente la salida de la ciudad de reporteros o editores en riesgo extremo.
- Establecer reglas de acceso a la oficina y áreas de trabajo como parte de la seguridad en el ambiente operativo.
- Proteger las computadoras y equipos móviles mediante una política de contraseñas y codificación de la información.
- Guardar una copia de respaldo de la información sensible o confidencial fuera de la oficina.
- Usar herramientas seguras en la navegación en Internet, comunicación en línea, plataformas de blog y redes sociales

PROTOCOLOS Y HERRAMIENTAS DE SEGURIDAD

ELABORACIÓN DE PROTOCOLOS

Como ya señalamos antes, la definición de los objetivos da lugar a un desglose de medidas preventivas o correctivas. Entre ellas se encuentran:

- Protocolos de prevención. Los protocolos definen paso por paso las acciones que hay que tomar para enfrentar una situación de riesgo. Así, puede haber protocolos para el desarrollo de fuentes periodísticas, investigación, cobertura de alto riesgo. Los protocolos de seguridad digital se refieren principalmente a la definición de operaciones para asegurar la protección de los datos y la comunicación entre dos partes.

- Planes de emergencia. Éstos son necesariamente correctivos e implican que los protocolos de seguridad fallaron para evitar el paso a niveles de alto riesgo. En el caso de riesgos extremos, los planes de emergencia requieren una acción rápida, posiblemente la suspensión inmediata de las operaciones de riesgo extremo y una evaluación posterior de la estrategia entera, así como de las vulnerabilidades, capacidades y recursos existentes.

Estos serían ejemplos de protocolos básicos a seguir:

Medidas básicas de seguridad digital general:

- Actualiza tu programa antivirus.
- Activa los *firewalls* o cortafuegos en tu computadora.
- Actualiza permanentemente todos los programas, sistemas operativos, navegadores y aplicaciones que tienen tus equipos.
- Protege tu equipo de sobre descargas eléctricas.
- Infórmate siempre de los nuevos viruses y programas maliciosos.
- Mantén una actitud de alerta permanente.
- Examina con cuidado la dirección electrónica de quien te envía un mensaje.
- Nunca abras un archivo que no esperabas. Si decides abrirlo, examínalo antes con tu programa antivirus.
- Nunca le des *click* a vínculos activos que te envían fuentes desconocidas o de baja confianza.
- Usa sólo contraseñas seguras.

Medidas básicas de seguridad digital en la redacción:

- Cierra tu computadora cuando te alejes de ella o protégela con una contraseña fuerte.
- Cierra tu navegador y desconecta tu equipo de internet si no navegas o si te alejas de tu equipo.
- Evalúa y elige los mejores parámetros de seguridad de tu navegador, sistema operativo, cuentas de correo electrónico, redes sociales y aplicaciones móviles.
- Respalda y organiza de mane-

ra permanente tu información.
- Usa carpetas encriptadas para guardar información confidencial o encripta el disco duro entero.
- Si usas equipo de la empresa en tu trabajo, evita usarlo para fines personales.
- Si estás en la red de la empresa, sigue las instrucciones de seguridad del departamento de IT (Tecnologías de la Información).
- Recuerda que en los equipos y redes de la empresa nada es privado.
- Acuerda con los directivos de tu empresa los medios de comunicación segura con fuentes confidenciales.
- Promueve la auditoría de seguridad digital y móvil en tu empresa.
- Presenta propuestas para elaborar un plan general de seguridad (amenazas, capacidades, vulnerabilidades, niveles de riesgo, objetivos, acciones y recursos).

Medidas básicas de seguridad digital fuera de la redacción:

- Sólo lleva el equipo necesario.
- Activa medidas de seguridad en tus dispositivos móviles en caso de pérdida.
- Nunca lleves tus archivos completos en tu computadora mientras cumples una asignación o realizas una cobertura.
- Deja los dispositivos de memoria USB o discos duros portátiles innecesarios a resguardo en la redacción.
- Lleva un dispositivo de memoria USB con el sistema de navegación Tor.
- Si no son necesarios, desactiva los sistemas GPS de tu teléfono celular o tableta.
- Desactiva el *Bluetooth* de tu teléfono celular si no lo usas.
- Lleva baterías adicionales para tu computadora, teléfono celular o tableta. Evitar usar equipos en las salas de prensa.
- De preferencia, evitar cargar la batería de tus equipos en salas de prensa u otros lugares públicos porque otros pueden acceder a tus equipos por esa vía[6].
- Evita acceder a redes inseguras de internet. De preferencia, accede a internet con un modem USB o con el recurso de HotSpot móvil de tu teléfono celular.
- Si consultas a fuentes confidenciales o intercambias datos o información confidencial con tu editor, usa formas encriptadas de comunicación.

Medidas básicas de seguridad digital en situaciones de riesgo

- Toma en cuenta y ejecuta un plan diseñado con anterioridad con tus editores.
- Manténte alerta de tu entorno y cualquier situación que obligue a un cambio en los protocolos de seguridad.
- Analiza si es necesario activar el GPS de tu celular para que seas localizado en caso de emergencia.
- Si llevas documentos o archivos que puedan poner en riesgo tu seguridad, analiza si es necesario alejarte del lugar.
- Si tomas fotografías de situaciones de riesgo, súbelas a un respaldo a la nube de internet. Bórralas de tu equipo o reemplaza la tarjeta de memoria de tu cámara o teléfono celular.
- Evita contactar a fuentes confidenciales en esos momentos. Tanto las fuerzas de seguridad como las criminales pueden tener activos sus equipos de interceptación de llamadas y datos.

6 Ver una explicación más detallada en este blog de seguridad: http://gcn.com/Blogs/CyberEye/2013/07/Blackhat-secure-travel-advice.aspx

SECCIÓN 6
Protección de equipos y contraseñas

PROTOCOLO DE PROTECCIÓN DE COMPUTADORAS

1. No mezcles lo personal con lo laboral

El daño probable puede ser mayor si los usuarios mezclan su información personal con la profesional. Perder información profesional afecta la seguridad del periodista y la de sus fuentes, pero perder información personal pone en riesgo la seguridad de amistades y familiares. Una separación clara es recomendable. Si necesitas llevar archivos personales, guárdalos en una carpeta encriptada con Truecrypt (Ver: http://www.truecrypt.org/).

Aquí puedes acceder a tutoriales para desarrollar carpetas con Truecrypt:

- http://www.slideshare.net/cfpdudg/cmo-cifrar-archivos-en-windows-y-mac-con-true-crypt
- https://securityinabox.org/es/truecrypt_principal

2. Cuida tu entorno laboral

Dimitri Vitaliev, un experto de Front Line Defenders que redactó el manual clásico de seguridad digital para defensores de derechos humanos[7], aconseja mantener un perímetro controlado de seguridad de las computadoras: que nadie extraño se acerque a ellas, que nadie sin autorización las use, que nadie ajeno pueda mirar la pantalla. Define de antemano los protocolos de seguridad como quién tiene acceso al lugar donde están los equipos, qué contraseña es fuerte y qué sucede cuando el usuario se aleja momentáneamente de la computadora.

Vitaliev aconseja también considerar los peores escenarios y evaluar el daño probable a la seguridad personal, de los colegas, de la reputación, e incluso de la estabilidad financiera, en caso de pérdida de control de la computadora. Los riesgos en ese tipo de casos son el robo del equipo, la confiscación del ordenador, el crackeo electrónico o el acceso a la computadora mediante la corrupción del personal encargado de custodiarla.

3. Revisa tu entorno físico

- Evita que un intruso entre con facilidad al edificio y llegue hasta tu espacio de trabajo.
- Impide que un intruso pueda acceder a la información de tu computadora cuando no estés.
- Analiza si alguien más ve tu pantalla cuando trabajas en tu computadora.
- No revises documentos confidenciales en su computadora si alguien más puede ver la pantalla.
- Apaga tu computadora, crea contraseñas de arranque, para regresar de un estado de reposo o quitar el protector de pantalla.
- Guarda tus dispositivos portátiles en lugares seguros si no los utilizas y no los abandones.
- Si tu equipo debe permanecer en una oficina asegúralo con candado si es posible.
- Mantener un control sistemático para controlar el acceso al área donde se ubica el equipo de cómputo que utiliza el periodista o el bloguero.

7 Para ver el Manual ve a http://www.frontlinedefenders.org/es/digital-security

- Actualiza todos los programas de la computadora, su sistema operativo y el navegador de Internet que utilizas.
- Actualiza el programa antivirus y fortalece tus contraseñas.
- Crea respaldos de la información en discos duros externos y guárdalos en un lugar seguro.
- Si tienes que guardar archivos electrónicos sensibles o confidenciales en tu computadora, crea una carpeta encriptada con Truecrypt. Ahí puedes ocultar tu carpeta en cualquier archivo y guardar tus documentos. (http://www.truecrypt.org/)
- Nadie más que tú debe usar tu computadora o dispositivo móvil. Nunca dejes tu computadora sola, abierta. Apágala o déjala dormir con una contraseña.
- Programa una contraseña de usuario y un protector de pantalla y nunca la compartas.
- Evitar el consumo de alimentos o líquidos junto a la computadora.
- Mantener actualizados todos los programas de cómputo que tiene el equipo.
- Si es una computadora compartida, crear una cuenta de usuario con una contraseña fuerte.
- No grabar las contraseñas en los sitios de Internet.
- Evitar la grabación o almacenamiento de información personal o fotos de familiares en la computadora.
- Mantener los archivos ordenados para que su localización sea fácil en caso necesario.
- Eliminar o guardar en otro lugar información que pueda ser utilizada en contra del reportero o bloguero o que despierte sospechas si un policía, militar o miembro de un grupo criminal inspecciona el equipo.

PROTOCOLO DE PROTECCIÓN DE CELULARES Y TABLETAS

- Elaborar una política de contraseñas para el teléfono celular que incluya: PIN, patrón, contraseña para iniciar el equipo y acceder a la tarjeta de memoria.
- Evitar el almacenamiento de la información de contacto de fuentes confidenciales en el teléfono que pueda estar en riesgo de pérdida o robo.
- Mantener asegurado el equipo móvil para reponer el aparato en caso de robo o extravío, así como borrar la información y bloquear el acceso a control remoto.
- Mantener al equipo móvil libre de información personal que pueda poner en riesgo al usuario, a sus colegas o amigos, o a su propia familia en caso de que pierda el control de sus dispositivos.
- Usar programas antivirus y mantener actualizadas todas las aplicaciones utilizadas para el trabajo del periodista o del bloguero.
- Eliminar las aplicaciones no necesarias o de simple esparcimiento.
- Llevar consigo siempre baterías de repuesto y mantener siempre cargada la batería del dispositivo móvil.
- Descargar las aplicaciones de navegación anónima en el móvil (Orbot y Orweb). Aquí puedes ver un tutorial: https://securityinabox.org/es/node/3001. Puedes descargar Orbot y Orweb en tu tienda de Google Play[8].
- Descargar la aplicación Ostel para encriptar el audio de las llamadas telefónica. Puedes descargar Ostel en el sitio del Proyecto Guardian[9].

8 Más información en https://guardianproject.info/apps/orbot/ y https://guardianproject.info/apps/orweb/
9 Más información de Ostel en https://guardianproject.info/apps/ostel/

PROTOCOLO DE PROTECCIÓN DE CONTRASEÑAS

- Elaborar una política de contraseñas seguras de arranque, pantalla protectora, así como las cuentas de administrador y usuario de las computadoras en riesgo.
- Las contraseñas deben ser mayores de 15 caracteres y combinar letras mayúsculas, minúsculas, números y signos.
- Las contraseñas deben cambiarse frecuentemente.
- Crear una política de contraseñas que defina el número mínimo de caracteres, prohibir el reciclamiento de contraseñas y definir el plazo máximo para renovarlas.
- Guardar en un programa de almacenamiento protegido (como Keepass http://keepass.info) las contraseñas anotadas en papeles, libretas, o archivos sin encriptación en la computadora. Aquí puedes ver un tutorial para instalar Keepass: https://securityinabox.org/es/keepass_principal. Las computadoras MacBook tienen el sistema de "Acceso de Llaveros" con la que puedes administrar las contraseñas y guardarlas en forma encriptada.
- Usar una contraseña distinta para cada cuenta de correo electrónico, redes sociales y sitios web.
- Crear Passphrases en lugar de Passwords. Las passphrases con conjuntos de cuatro o cinco palabras o contraseñas que funcionan juntas para abrir documentos, aplicaciones, programas o redes sociales. Aquí puedes ver un tutorial de cómo crear una passphrase con un dado: http://world.std.com/%7Ereinhold/diceware_en_espanolA.htm
- Medir la fortaleza de las contraseñas en sitios de Internet: www.passwordmeter.com, https://howsecureismypassword.net, https://www.microsoft.com/en-au/security/pc-security/password-checker.aspx
- Usar el programa Truecrypt para usar una contraseña en el arranque de la computadora y encriptar el disco duro interno.

Puedes revisar este tutorial para la protección de equipos:

- http://www.slideshare.net/latinointx/proteccion-de-equipos-documentos-y-contrasenas

SECCIÓN 7
Almacenamiento y protección de la información

Los periodistas suelen almacenar grandes cantidades de archivos electrónicos sin separar los archivos con información confidencial de los que no tienen datos que requieran protección especial.

Ese almacenamiento desorganizado de los archivos puede ser un factor de riesgo si perdemos el control de la computadora o del equipo móvil.

Quizá uno de los ejemplos más extremos de esa situación es el secuestro de dos periodistas[10] en Reynosa, Tamaulipas que cubrían el enfrentamiento entre los carteles del Golfo y de los Zetas en la primavera de 2010. Uno de los reporteros llevaba en su computadora fotografías tomadas en una ceremonia militar que había ocurrido días atrás en la ciudad de México. Al revisar las computadoras de los periodistas secuestrados, los secuestradores interpretaron esas fotografías como una muestra de que los reporteros trabajaban para los Zetas, el grupo criminal que fue integrado por ex miembros del Ejército mexicano. De alguna forma, el reportero pudo demostrar su condición profesional y con eso evitar el asesinato de él y su compañero.

El ejemplo nos ofrece varias enseñanzas que los periodistas que cubren situaciones de alto riesgo tienen que recuperar.

- La primera es que hay que separar los archivos con información sensible de los que no la tienen. La información sensible puede abarcar desde archivos de Word con nombres, teléfonos o correos electrónicos de fuentes de información hasta notas escritas con datos acerca de la corrupción de funcionarios públicos. Otros documentos con datos de menor confidencialidad deben estar separados.
- Los documentos que el periodista considere confidenciales deben guardarse en carpetas encriptadas con Truecrypt, un programa gratuito disponible en Internet que permite la creación de drives encriptados que sólo pueden abrirse con una contraseña. Truecrypt permite la creación de carpetas encriptadas ocultas en otro documento como una fotografía, un documento de Power Point o un documento de Word. En esas carpetas pueden guardarse fotografías con información que en otros contextos pueden ser motivo de riesgo para los periodistas.
- Los periodistas deben viajar con computadoras y celulares "limpios" de información. En caso de pérdida, robo o confiscación, el periodista puede asegurar que ningún dato confidencial está en riesgo. Eso significa que antes de salir a realizar la cobertura, los periodistas deben mover las carpetas encriptadas a otras computadoras seguras y viajar con computadoras vacías. Los periodistas pueden mantener información no sensible en sus computadoras.
- En el caso de periodistas que trabajen para un medio, los reporteros pueden llevar computadoras de la empresa que estén especialmente preparadas para la cobertu-

10 Ver: http://homozapping.com.mx/2012/01/testimonio-de-un-periodista-sobreviviente-en-reynosa/

ra de situaciones de riesgo. Los periodistas deben recordar que pueden encontrarse inesperadamente con situaciones de alto riesgo como retenes militares, policiales o criminales donde sus equipos pueden ser sujetos a la confiscación y revisión. En el caso de los fotógrafos, el riesgo es mayor pues suelen emplear sus equipos propios para la cobertura.

- Si crean archivos sensibles durante la cobertura, éstos deben ser almacenados en carpetas creadas con Truecrypt y ocultar en una fotografía u otro archivo similar.
- Los periodistas también pueden crear carpetas con Truecrypt y almacenarlas en DropBox (https://www.dropbox.com) o Google Drive (https://drive.google.com/). De esta manera, los archivos siempre estarán disponibles y protegidos con una encriptación doble.

PROTOCOLO DE PROTECCIÓN DE DOCUMENTOS

Los periodistas suelen tener ahora una gran cantidad de documentos electrónicos que van acumulando en el transcurso de sus investigaciones. El problema no es sólo cómo administrar esa información y tenerla siempre disponible y organizada, sino también cómo protegerla.

En el contexto de situaciones de alto riesgo, ahora se ha vuelto indispensable que los periodistas desarrollen habilidades para proteger su información, sobre todo aquella que incluye datos sensibles o confidenciales. Los datos que guardan periodistas de investigación suelen estar relacionados con evidencias de corrupción de funcionarios públicos o asuntos relacionados con la delincuencia organizada. Esa es la razón por la que los atacantes de periodistas suelen apoderarse de sus computadoras o dispositivos móviles (celulares o tabletas).

Una de las formas de protección de nuestros documentos es la codificación o encriptación[11], que implica la conversión de un documento legible a uno ilegible para quien no tiene la contraseña para decodificarlo. Si por alguna razón perdemos la memoria USB donde teníamos nuestro documento, o si perdemos la computadora, el teléfono o la tableta con ese documento, las personas no podrán leer el documento si no tienen la contraseña de decodificación.

La necesidad de encriptar la información alcanza también documentos que en un contexto normal no tendrían por qué generar una situación de riesgo. Los especialistas en seguridad de la información recomiendan que siempre debemos trabajar con la idea de que todos los escenarios son posibles, incluidos los catastróficos que, en este caso, podrían consistir en la pérdida del control de toda la información que tenemos. Si algo así pasara, no solamente nuestra información estaría en riesgo, sino también la seguridad de las fuentes periodísticas.

La protección de documentos incluye la actualización de programas antivirus y el respaldo periódico de la información en discos duros externos.

Aquí te ofrecemos una guía para encriptar tus documentos Word, que son normalmente los documentos con los que trabaja un periodista.

- http://www.slideshare.net/latinointx/codificacion-de-documentos-de-word

11 Para una explicación breve de la encriptación ve: http://www.uoc.edu/inaugural01/esp/encriptacion.html

SECCIÓN 8
Navegación anónima en internet

La navegación anónima es fundamental para periodistas o reporteros ciudadanos que están investigando situaciones de riesgo o casos de corrupción. La navegación anónima consiste en disfrazar el código IP (Internet Protocol) que el proveedor de servicios de internet asigna cuando un navegador (web browser) se conecta con un Servidor (internet server). Este número único está asociado con los datos de identificación del cliente del proveedor de servicios de internet.

En el caso de los IP que son asignados a la navegación en las redacciones de los diarios, revistas, medios en línea o estaciones de radio o TV, el código está asociado a los datos de la empresa. Sin embargo, cuando el periodista navega desde su casa o desde su teléfono celular o tableta, es posible que el IP esté entonces asociado con sus datos personales.

De esa manera, los funcionarios públicos corruptos, las empresas que puedan ser afectadas por la investigación periodística, o los grupos criminales, podrían conocer la identidad de los periodistas a través del rastreo del IP.

El IP también puede ser revelado en los encabezados (*headers*) de correo electrónicos inseguros.

De cualquier manera, el periodista o reportero ciudadano puede estar interesado en proteger su identidad a través de la navegación anónima. Una de las herramientas disponibles es el navegador de Tor (https://www.torproject.org).

La plataforma Tor utiliza una red de servidores proxy que prestan su IP para enmascarar el IP original del usuario de internet. Cuando el periodista o reportero ciudadano está conectado a la red Tor y abre un nuevo sitio de internet, el servidor proxy usa su propio IP, en lugar del IP de la computadora del usuario, para pedir los datos de un nuevo sitio a otro servidor. De esta manera, la identidad del usuario queda protegida.

En teléfonos celulares con sistema operativo Android, la plataforma Tor puede ser usada a través de las aplicaciones Orbot y Orweb.

Conviene enrutar el teléfono

celular para aprovechar todas las ventajas de Tor en celulares, entre ellas, el uso anónimo de todas las aplicaciones que conectan al celular con internet.

La protección de la privacidad incluye también el uso del prefijo https en todos los sitios donde haya que escribir una contraseña y el cuidado para no abrir sitios web con contraseña en redes inalámbricas abiertas, sin contraseña de acceso.

Algunos reporteros han tenido que usar computadoras o acceder a redes de internet en oficinas de prensa gubernamentales para enviar información cuando la batería de sus equipos está agotada. Por esa razón, la alimentación de baterías es esencial en la cobertura periodística.

PROTOCOLOS DE NAVEGACIÓN ANÓNIMA

- Utilizar sitios de internet que tengan el prefijo https. Ese prefijo encripta la interacción entre el navegador de internet y el servidor.
- Usar la herramienta https everywhere en el navegador Firefox.
- Usar la plataforma TOR cada vez que estemos haciendo una investigación en línea sobre temas complicados. Aquí tienes un tutorial sobre cómo descargar la plataforma Tor en tu computadora: http://www.slideshare.net/latinointx/manual-para-usar-tor
- Usar Redes Privadas Virtuales (VPN por sus siglas en inglés) para navegar en internet. Las VPN se utilizan como un túnel para proteger la privacidad de la navegación en internet.
- Usar otras herramientas como Anonymox en el navegador Firefox.
- Evitar la grabación del historial de navegación mientras usamos el navegador de TOR.
- Utilizar sólo el acceso encriptado a internet inalámbrico.
- No abrir cuentas que requieran contraseñas en redes de acceso inalámbrico abierto (sin encriptar) a internet.
- Usar modems USB para acceder a Internet mientras estamos fuera de la oficina.
- Usar el ambiente TOR con Orbot y Orweb en la navegación de internet en celulares y tabletas.

Aquí puedes revisar un tutorial sobre la navegación anónima en internet:

- http://www.slideshare.net/latinointx/proteccin-de-la-privacidad-y-navegacin-annima-en-internet

SECCIÓN 9
Protección de las comunicaciones digitales

Con las revelaciones recientes sobre el espionaje electrónico realizado por agencias de inteligencia estadounidense y la adquisición de equipos de espionaje por parte de gobiernos y empresas privadas de espionaje, sabemos que la interceptación de toda la actividad electrónica de los periodistas es una práctica frecuente en zonas de guerra.

El riesgo inherente a esta violación de la privacidad aumenta cuando quien espía las comunicaciones y en general toda la actividad electrónica de los periodistas, es el crimen organizado o los funcionarios públicos asociados con grupos criminales.

Los periodistas y reporteros ciudadanos deben entonces proteger sus comunicaciones para que ninguna información confidencial sea puesta en riesgo.

Eso incluye la creación de cuentas de correo electrónico seguras, la encriptación de chats o mensajería instantánea, así como la encriptación de mensajes de texto y conversaciones vía telefónica.

PROTOCOLO DE COMUNICACIÓN SEGURA

- Elaborar una política de comunicación que incluya vías abiertas y cerradas de comunicación cuando la naturaleza del tema sea delicada y sensible. Eso significa que las vías abiertas serán no encriptadas y servirán para enviar comunicación no confidencial, mientras que las vías cerradas serán usadas para transmitir sólo información confidencial. En algunos casos, podría ser conveniente usar vías abiertas no encriptadas para enviar información confidencial cuya divulgación no pone en riesgo la seguridad de las personas.
- Usar herramientas de codificación en la transmisión de mensajes vía correos electrónicos. El servicio de Hushmail (https://www.hushmail.com) encripta el contenido de los mensajes. Hushmail tiene la ventaja de que no pide datos personales para abrir una cuenta. Sin embargo, la compañía sí tiene acceso a nuestra contraseña. Otra desventaja de Hushmail es que los usuarios necesitan abrir sus cuentas por lo menos una vez cada tres semanas para evitar que las cuentas de Hushmail sean desactivadas. Actualmente, Hushmail realiza un cargo para reactivar cuentas suspendidas.
- Otra forma de proteger el contenido de los correos electrónicos es el uso de una herramienta gratuita y sencilla de usar en internet: infoencrypt (http://infoencrypt.com) . Esta herramienta nos permite copiar y pegar un texto previamente escrito y encriptarlo mediante una contraseña. El texto encriptado puede a su vez copiarse y pegarse en el cuerpo del mensaje electrónico. El reto es enviar la contraseña al destinatario. Infoencrypt recomienda siempre enviar las contraseñas por una vía distinta.
- Existen otras alternativas accesibles y sin costo para proteger la comunicación entre el periodista, sus fuentes o sus editores. El servicio de Riseup (https://help.riseup.net) encripta el mensaje electrónico en el tránsito desde el remitente hasta el destinatario. Riseup.net no incluye el IP en sus encabezados ni guardar las contraseñas elegidas por los usuarios. Con esas características, Riseup.net es una de

las mejores posibilidades para proteger las comunicaciones del periodista.

- Evitar la anotación de información personal en las cuentas de correo electrónico, redes sociales y plataformas de blogueo.
- Utilizar cuentas de correo electrónico obtenidas desde la plataforma de Tor para abrir blogs anónimos o cuentas de redes sociales también anónimas.
- Sólo acceder a esas cuentas anónimas desde el ambiente de navegación anónima Tor.
- Utilizar sólo cuentas de correo electrónico que ocultan el IP de los usuarios de internet en los encabezados del mensaje.
- Utilizar un procedimiento de doble autenticación (contraseña más código enviado al teléfono celular) para abrir las cuentas de correo electrónico, mensajería instantánea o redes sociales.

PROTOCOLO DE SEGURIDAD DEL CHAT

Los periodistas y reporteros ciudadanos han descubierto que la mensajería instantánea es una de las formas más rápidas y accesibles para comunicarse con las fuentes, colegas o editores.

Desafortunadamente esas plataformas no son seguras porque transmiten los mensajes en texto plano sin encriptar. Aunque las comunicaciones por esos medios son rápidas, pueden ser fácilmente interceptadas y leídas por otras personas.

Existen sin embargo otras herramientas que nos ayudan a encriptar las plataformas de chateo o mensajería instantánea. Esas herramientas como Pidgin (http://www.pidgin.im) en sistemas operativos Windows o Adium (https://adium.im) en iOS, usan un recurso llamado OTR (Off The Record) para encriptar servicios de mensajería instantánea como Google Chat, Facebook Chat, Yahoo Messenger o Microsoft Messenger (MSN Messenger).

- Usa una combinación de chats inseguros y seguros. Puedes usar por ejemplo Whatsapp y Google Talk encriptado para reducir la atención de espías potenciales a tus conversaciones electrónicas.

SEGURIDAD EN MENSAJES DE TEXTO

Los mensajes de texto son particularmente vulnerables porque pueden ser leídos por cualquier persona que los intercepte. Una manera accesible de encriptar los mensajes de texto es TextSecure, una aplicación para encriptar los mensajes de texto en dispositivos móviles que usan Android.

La aplicación es gratuita y puedes bajarla en la tienda de Google Play. Aquí te encuentras con una guía para utilizar TextSecure: https://securityinabox.org/es/node/3003

ENCRIPTACIÓN DE LLAMADAS TELEFÓNICAS

El Proyecto Guardián ha desarrollado la herramienta llamada Ostel (https://guardianproject.info/apps/ostel/) para encriptar las comunicaciones telefónicas. Funciona en los sistemas operativos de Android, iPhone, Blackberry, Nokia, PC, Mac y Linux.

- https://ostel.me

SECCIÓN 10
Uso seguro de redes sociales

PROTOCOLO DE PROTECCIÓN DE TWITTER

- Crear un sistema de doble autenticación (contraseña más código numérico enviado al teléfono celular) para abrir la cuenta de Twitter https://twitter.com).
- Usar HTTPS mientras trabajas en Twitter.
- Si abres una cuenta de Twitter anónima evita anotar tus datos reales de identidad. Sólo escribe datos ficticios que no estén relacionados contigo.
- Evita escribir datos personales en tu actividad en Twitter que revelen patrones de conducta personal como hábitos cotidianos, lugares que frecuentas, personas cercanas, afectos importantes, así como inclinaciones políticas.
- De manera normal, evitar geolocalizar los tuits. Eso ayuda a no revelar rutinas diarias.
- Si te sientes en riesgo en una cobertura noticiosa, activa la geolocalización de los tuits. Eso te ayudará a recibir ayuda rápida en caso de emergencia.
- Investiga las aplicaciones relacionadas con Twitter y sólo usa aquellas que tienen buena reputación.
- Elimina las aplicaciones que tengan acceso a tus mensajes directos en Twitter. Eso mantiene protegidos los mensajes.
- Cryptoperiodismo recomienda usar una contraseña distinta para cada una de las redes sociales que usa el periodista o el bloguero.

PROTOCOLO DE PROTECCIÓN DE FACEBOOK

- Permanece atento a los cambios en las políticas de privacidad pues Facebook cambia constantemente los parámetros de privacidad.
- Acepta solicitudes de amistad solo de personas que conoces.
- Crea grupos de amistades con diferentes niveles de acceso a tu muro, biografía, gustos, fotos y contactos.
- Si aceptas una solicitud de amistad de una persona que desconoces, colócala en un grupo con los menores privilegios posibles.
- Mantén tus contactos privados. Esta medida sólo muestra contactos compartidos a los demás.
- Evita subir información personal que pueda poner en riesgo tu integridad o la de tu familia.
- Acepta aplicaciones con buena reputación corroborada.
- Toma en cuenta que todo lo que subes a tu muro puede ser público con herramientas de búsqueda.
- Cuida lo que subes a Facebook. Considera que si una persona le "gusta" una foto o comentario tuyo, todos sus contactos pueden ver lo que tú subiste a Facebook.
- Elimina los tags de tu rostro en las fotografías que otros suben a sus muros en Facebook. La red social tiene un mecanismo de reconocimiento facial automatizado y puede poner tu nombre a fotografías que correspondan a tu perfil físico.
- Planea cuidadosamente lo que subes a Facebook.
- Sigue la página de Facebook Security: https://www.facebook.com/security.
- Revisa la configuración de seguridad de tu cuenta de Facebook y adopta las siguientes medidas: a) Activa la navegación segura, b) Activa las notificaciones por correo electrónico, c) Establece como paso obligado un código de seguridad al iniciar sesión desde un navegador desconocido, d) Activa el generador de códigos, e) limita los dispositivos reconocidos para evitar que otras personas accedan a tu cuenta, f) revisa las sesiones activas y elimina aquellas que no reconozcas.

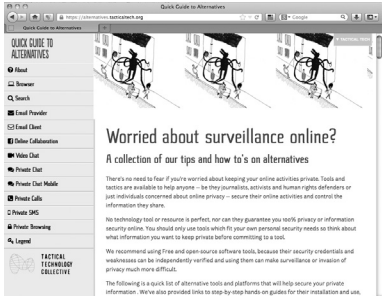
SECCIÓN 11
Sitios web

PERIODISTAS EN RIESGO
https://periodistasenriesgo.crowdmap.com/main
En español
Organizaciones: International Center for Journalists, Freedom House
Mapa de agresiones a periodistas y blogueros en México. Incluye el registro de agresiones digitales.

MI MÉXICO TRANSPARENTE
http://mimexicotransparente.com
En español
Organizaciones: International Center for Journalists, Freedom House
Análisis de las tendencias de agresiones a periodistas y blogueros en México. Forma parte del proyecto general de uso de mapas digitales para reportar crimen y corrupción.

IJNET
En español
Organización: International Center for Journalists
Blog de Jorge Luis Sierra sobre seguridad digital.

SECURITY IN A BOX
https://securityinabox.org
En español
Organizaciones: Tactical Technology Collective y Frontline Defenders
Este sitio web reúne prácticamente todas las herramientas y programas de seguridad digital. Incluye instrucciones y tutoriales.

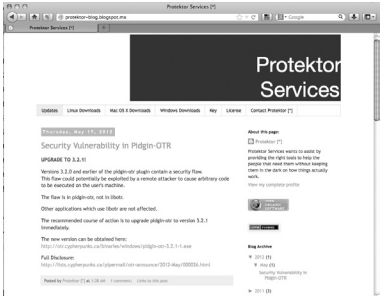


QUICK GUIDE TO ALTERNATIVES
https://alternatives.tacticaltech.org
En inglés
Organización: Tactical Technology Collective
Este sitio web reúne herramientas y programas de seguridad digital con una explicación breve de para qué sirve cada una.

THE GUARDIAN PROJECT
https://guardianproject.info
En inglés
Organización: The Guardian Project
El grupo ha producido aplicaciones de seguridad digital para dis-

positivos móviles como teléfonos celulares y tabletas: Orbot, Orweb, Gibberbot, ObscuraCam y Ostel.

THE TOR PROJECT
https://www.torproject.org
En inglés
Ofrece en forma gratuita la plataforma Tor para proteger la privacidad del usuario y vigilancia en internet y el análisis de tráfico.



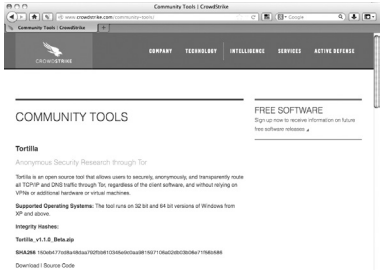
SERVICIOS DE PROTECCIÓN
http://protektor-blog.blogspot.com
En inglés
Organización: Protektor
Blog sobre seguridad digital

FUNDACIÓN FRONTERA ELECTRÓNICA
https://www.eff.org
En inglés
Organización: Electronic Frontier Foundation
Sitio web dedicado a la protección de la privacidad. Creadores de Https Everywhere, la herramienta de encriptación de la navegación en internet. Incluye blogs sobre las principales noticias relacionadas con la privacidad en línea.

LIBERTAD DE INTERNET
http://www.freedomhouse.org/program/internet-freedom
En inglés
Organización: Freedom House
Recursos sobre entrenamiento, campañas y reportes sobre la libertad de internet y la defensa de la seguridad digital.

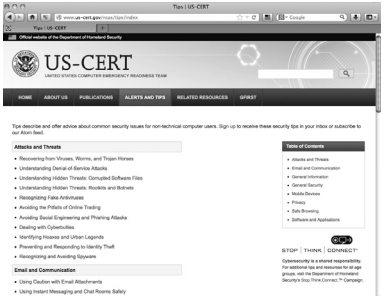
ROBOT ONO
https://onorobot.org/#
En inglés
Organización: Tactical Tech Collective
Serie de animaciones sobre Ono Robot, un amigo virtual que cuida de tu seguridad digital.

SAFETY ON THE LINE: EXPOSING THE MITH OF MOBILE COMMUNICATION SECURITY
http://www.freedomhouse.org/report/special-reports/safety-line-exposing-myth-mobile-communication-security
En inglés
Organización: Freedom House
Evaluación de la seguridad de la comunicación en teléfonos, plataformas y aplicaciones móviles en 12 países.



CROWDSTRIKE: *COMMUNITY TOOLS*
http://www.crowdstrike.com/community-tools/
En inglés
Organización: Crowdstrike.
Presenta *Tortilla*, una herramienta que permite un uso de la navegación anónima más seguro de Tor. También ofrece otras herramientas de seguridad.

CRYTOPARTY
http://www.cryptoparty.in
En inglés
Organización: Criptoparty
Organización de reuniones a nivel global para diseminar las herramientas de encriptación en la navegación de internet y la comunicación digital.



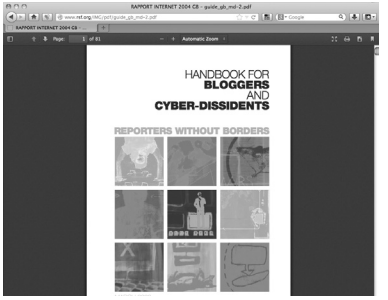
U.S. CERT. UNITED STATES COMPUTER EMERGENCY READINESS TEAM
http://www.us-cert.gov/ncas/tips/index
En inglés
Organización: Departamento de Seguridad Interna.
Ofrece tips de seguridad comunes para usuarios no especializados.

SECCIÓN 12
Otros manuales

SEGURIDAD DIGITAL Y PRIVACIDAD PARA DEFENSORES DE DERECHOS HUMANOS
http://www.frontlinedefenders.org/digital-security
En español
Organización: Front Line Defenders
Manual de seguridad digital.

BLOGUEO ANÓNIMO CON WORDPRESS Y TOR
http://advocacy.globalvoicesonline.org/projects/guide/
En inglés
Organización: Global Voices
Manual para bloguear en forma anónima

BLOGUEA POR UNA CAUSA
http://advocacy.globalvoicesonline.org/projects/guide-blog-for-a-cause/blog-por-una-causa/
En español
Organización: Global Voices
Quía para usar blogs para defender una campaña por la justicia social.



MANUAL PARA BLOGUEROS Y CIBER-DISIDENTES
http://www.rsf.org/IMG/pdf/guide_gb_md-2.pdf
En inglés
Organización: Reporteros Sin Fronteras
Manual para el uso de blogs en sociedades represivas, incluye recomendaciones de seguridad digital.

GUÍA PARA EVADIR LA CENSURA EN INTERNET
http://www.civisec.org/guides/everyones-guides
En inglés
Organización: ClvicSec

SPEAKSAFE
http://speaksafe.internews.org
En español
Organización: Internews
Manual de seguridad digital

MANUAL DE SEGURIDAD PARA PERIODISTAS
http://www.cpj.org/es/2012/04/manual-de-seguridad-para-periodistas-del-cpj.php
En español
Organización: Comité para la Protección de Periodistas
Manual de seguridad para periodistas que contiene recomendaciones de seguridad digital.

GUIDE TO SAFELY AND SECURELY PRODUCING MEDIA
http://smallworldnews.tv/guide/
En inglés
Organización: Small World News
Manual para producir medios con recomendaciones de seguridad.

CRIPTOPERIODISMO
http://cryptoperiodismo.org
En español
Organización: Pablo Mancini y Nelson Fernández
Manual sobre seguridad digital para periodistas.

SURVEILLANCE SELF DEFENSE
https://ssd.eff.org
En inglés
Organización: Electronic Frontier Foundation
Sitio sobre las leyes y tecnología de vigilancia electrónica gubernamental en Estados Unidos y las medidas apropiadas para evaluar el riesgo y tomar pasos para defenderse contra la vigilancia.

MACARTHUR
The John D. and Catherine T. MacArthur Foundation

Este manual se realizó con el apoyo de la Fundación MacArthur.

FREEDOM HOUSE
MÉXICO

STAFF

MARICLAIRE ACOSTA URQUIDI
Directora

CHANTAL PASQUARELLO
Directora Adjunta

DARÍO FRITZ
Oficial Senior de Programas

MARIO CARMONA
Oficial de Programas

TANIA TURNER
Analista de Monitoreo y Evaluación

GRACIELA SILVA
Gerente de Administración y Finanzas

GLORIA MORALES
Coordinadora de Gestión

Guanajuato 224 – 203
Colonia Roma
Delegación Cuauthémoc CP. 06700
México, Distrito Federal
Teléfonos: 5264 7072 / 0442
www.freedomhouse.org

©Derechos Reservados
Freedom House Oficina México
Octubre, 2013

Diseño: Dijard Studio
www.dijard.com